GDPR03 - Data Security and Data Retention Policy and Procedure

Category: GDPR **Sub-category:** Policies

Policy Review Sheet

Review Date: 07/03/18 **Policy Last Amended:** 07/03/18

Next planned review in 12 months, or sooner as required.

Note: The full policy change history is available in your online management system.

Business Impact:	Low	Medium	High	Critical
			X	
These changes require action as soon as possible. Changes include fixed implementation dates which are detailed within the policy.				

Reason for this review:	New Policy
Were changes made?	Yes
Summary:	This policy explains the key GDPR principles relating to data security and data retention and will assist organisations to review whether their current policies and procedures are sufficient, or whether they need updating.
Relevant Legislation:	• General Data Protection Regulation 2016 • Data Protection Bill 2017
Underpinning Knowledge - What have we used to ensure that the policy is current:	• GOV.UK, (2018), *About the IG Toolkit*. [Online] Available from: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf [Accessed: 07/03/2018] • Department of Health & Social Care and NHS England, (2018), *2017/18 Data Security and Protection Requirements*. [Online] Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf [Accessed: 07/03/2018] • Home Office, (2018), *An Employer's Guide to Right to Work Checks*. [Online] Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/638349/Employer_s_guide_to_right_to_work_checks_-August_2017.pdf [Accessed: 07/03/2018] • NHS DIGITAL,, (2018), *Records Management Code of Practice for Health and Social Care 2016*. [Online] Available from: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016 [Accessed: 07/03/2018]
Suggested action:	• Notify relevant staff of changes to policy • Training sessions • Discuss in team meetings • Discuss in supervision sessions • Impact assessment/action plan • Confirm relevant staff understand the content of the policy • Add the policy to the planned team meeting agendas • Encourage sharing the policy through the use of the QCS App

GDPR03 - Data Security and Data Retention Policy and Procedure

This page is deliberately left blank

GDPR03 - Data Security and Data Retention Policy and Procedure

1. Purpose

1.1 The purpose of this policy is to ensure that The Knares Medical Practice Basildon and all its staff understand the principles set out in GDPR in relation to data retention and data security.

1.2 By reviewing this policy, The Knares Medical Practice Basildon will be able to consider appropriate retention periods for the personal data it processes.

1.3 This policy will enable The Knares Medical Practice Basildon and all staff working at The Knares Medical Practice Basildon to review the policies and procedures they have in place to ensure that personal data they process is kept secure and properly protected from unlawful or unauthorised processing and accidental loss, destruction or damage.

1.4 To support The Knares Medical Practice Basildon in meeting the following Key Lines of Enquiry:

Key Question	Key Line of Enquiry (KLOE)
WELL-LED	HW4: Are there clear responsibilities, roles and systems of accountability to support good governance and management?
WELL-LED	HW5: Are there clear and effective processes for managing risks, issues and performance?

1.5 To meet the legal requirements of the regulated activities that The Knares Medical Practice Basildon is registered to provide:

- General Data Protection Regulation 2016
- Data Protection Bill 2017

2. Scope

2.1 The following roles may be affected by this policy:

- All staff

2.2 The following people may be affected by this policy:

- Patients

2.3 The following stakeholders may be affected by this policy:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 The objective of this policy is to enable The Knares Medical Practice Basildon to determine whether its data retention and data security policies are GDPR compliant and, if not, to update them prior to 25 May 2018.

3.2 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

GDPR03 - Data Security and Data Retention Policy and Procedure

4. Policy

4.1 Data Retention

As a general principle, The Knares Medical Practice Basildon will not keep (or otherwise process) any personal data for longer than is necessary. If The Knares Medical Practice Basildon no longer requires the personal data once it has finished using it for the purposes for which it was obtained, it will delete the personal data.

4.2 The Knares Medical Practice Basildon may have legitimate business reasons to retain the personal data for a longer period. This may include, for example, retaining personnel records in case a claim arises relating to personal injury caused by The Knares Medical Practice Basildon that does not become apparent until a future date. The Knares Medical Practice Basildon should consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by The Knares Medical Practice Basildon will, for example, affect the likelihood of The Knares Medical Practice Basildon needing to rely on records at a later date.

4.3 The Knares Medical Practice Basildon may be required to retain personal data for a specified period of time to comply with legal or statutory requirements. These may include, for example, requirements imposed by HMRC in respect of financial documents, or guidance issued by the Home Office in respect of the retention of right to work documentation (see "Underpinning Knowledge" section).

4.4 The Knares Medical Practice Basildon understands that claims may be made under a contract for 6 years from the date of termination of the contract, and that claims may be made under a deed for a period of 12 years from the date of termination of the deed. The Knares Medical Practice Basildon may therefore consider keeping contracts and deeds and documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed plus 6 and 12 years respectively.

4.5 The Knares Medical Practice Basildon will consider how long it needs to retain HR records. The Knares Medical Practice Basildon may choose to separate its HR records into different categories of personal data (for example, health and medical information, holiday and absence records, next of kin information, emergency contact details, financial information) and specify different retention periods for each category of personal data. The Knares Medical Practice Basildon recognises that determining separate retention periods for each element of personal data may be more likely to comply with GDPR.

The Knares Medical Practice Basildon may decide, however, that separating its HR records into different elements is not practical, and that it can determine a sensible period of time for which to keep the HR records in their entirety. The period of time that is appropriate may depend on the likelihood of a claim arising in respect of that employee in the future. If, for example, The Knares Medical Practice Basildon is concerned that an employee may suffer personal injury as a result of its employment with The Knares Medical Practice Basildon, The Knares Medical Practice Basildon may choose to retain its HR records for a significant period of time. If any such claim is unlikely, The Knares Medical Practice Basildon may choose to retain its files for 6 or 12 years (depending on whether the arrangement entered into between The Knares Medical Practice Basildon and the employee is a contract or a deed).

4.6 The Knares Medical Practice Basildon will consider for how long it is required to keep records relating to Patients. In doing so, The Knares Medical Practice Basildon will consider the data retention guidelines provided by the NHS, if applicable. Those guidelines can be accessed by using the link in the "Further Reading" section.

If the NHS guidelines don't apply to The Knares Medical Practice Basildon, The Knares Medical Practice Basildon will determine an appropriate retention policy for Patient personal data. The Knares Medical Practice Basildon may choose to retain personal data for at least 6 years from the end of the provision of services to the Patient, in case a claim arises in respect of the services provided.

4.7 Irrespective of the retention periods chosen by The Knares Medical Practice Basildon, The Knares Medical Practice Basildon will ensure that all personal data is kept properly secure and protected for the period in which it is held by The Knares Medical Practice Basildon. This applies in particular to special categories of data.

4.8 The Knares Medical Practice Basildon will record all decisions taken in respect of the retention of personal data. The Knares Medical Practice Basildon recognises that if the ICO investigates The Knares Medical Practice Basildon's policies and procedures, a written record of the logic and reasoning behind the retention periods adopted by The Knares Medical Practice Basildon will assist The Knares Medical Practice Basildon's position.

GDPR03 - Data Security and Data Retention Policy and Procedure

4.9 The Knares Medical Practice Basildon will implement processes for effectively destroying and/or deleting personal data at the end of the relevant retention period. The Knares Medical Practice Basildon will consider whether personal data stored on computers, including in emails, is automatically backed up and how to achieve deletion of those backups or ensure that the archived personal data is automatically deleted after a certain period of time. The Knares Medical Practice Basildon will consider circulating guidance internally to encourage staff to regularly delete their emails.

The Knares Medical Practice Basildon will introduce policies relating to the destruction of hard copies of documents, including by placing the documents in confidential waste bins or shredding them.

4.10 Data Security

The Knares Medical Practice Basildon will take steps to ensure the personal data it processes is secure, including by protecting the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.11 The Knares Medical Practice Basildon understands that all health and care organisations, as detailed below, are required to comply with the Information Governance Toolkit (the "IG Toolkit"). The IG Toolkit will be replaced from April 2018 with the new Data Security and Protection Toolkit. A link to an explanatory guidance note is included in the "Underpinning Knowledge" section. Compliance with the IG Toolkit and the Data Security and Protection Toolkit will facilitate compliance with GDPR.

The Knares Medical Practice Basildon understands that the following types of organisation must comply with the Data Security and Protection Toolkit:

- Organisations contracted to provide services under the NHS Standard Contract
- Clinical Commissioning Groups
- General Practices that are contracted to provide primary care essential services
- Local authorities and social care providers must take a proportionate response to the new toolkit:
    - Local authorities should comply with the toolkit where they provide adult social care or public health and other services that receive services and data from NHS Digital, or are involved in data sharing across health and care where they process confidential personal data of Patients who access health and adult social care services
    - Social care providers who provide care through the NHS Standard Contract should comply with the toolkit. It is also recommended that social care providers who do not provide care through the NHS Standard Contract consider compliance with the new toolkit from April 2018, which will help to demonstrate compliance with the ten security standards and GDPR

4.12 The Knares Medical Practice Basildon will implement and embed the use of policies and procedures to ensure personal data is kept secure. The suggestions below apply in addition to the steps The Knares Medical Practice Basildon is required to take pursuant to the IG Toolkit and the new Data Security and Protection Toolkit, if the toolkits apply to The Knares Medical Practice Basildon.

For paper documents, these will include, where possible:

- Keeping the personal data in a locked filing cabinet or locked drawer when it is not in use
- Adopting a "clear desk" policy to ensure that personal data is not visible or easily retrieved
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Redacting personal data from documents where possible
- Ensuring documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period

For electronic documents, the measures taken by The Knares Medical Practice Basildon will include, where possible:

- Password protection or, where possible, encryption
- Ensuring documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Ensuring ongoing confidentiality, integrity and reliability of systems used online to process personal data (this may require a review of IT systems and software currently used by The Knares Medical Practice Basildon)
- The ability to quickly restore the availability of and access to personal data in the event of a technical incident (this may require a review of IT systems and software currently used by The Knares Medical

Practice Basildon)
- Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipients

The Knares Medical Practice Basildon will ensure that all business phones, computers, laptops and tablets are password protected.

The Knares Medical Practice Basildon will encourage staff to avoid, storing personal data on portable media such as USB devices. If the use of portable media can't be avoided, The Knares Medical Practice Basildon will ensure that the devices it uses are encrypted or password protected and that each document on the device is encrypted or password protected.

4.13 The Knares Medical Practice Basildon will implement guidance relating to the use of business phones and messaging apps. The Knares Medical Practice Basildon understands that all personal data sent via business phones, computers, laptops and tablets may be captured by GDPR, depending on the content and context of the message. As a general rule, The Knares Medical Practice Basildon will ensure that staff members only send personal data by text or another messaging service if they are comfortable that the content of the messages may be captured by GDPR and may be provided pursuant to a Subject Access Request (which will be explained in more detail in a future policy).

4.14 The Knares Medical Practice Basildon will ensure that all staff are aware of the importance of keeping personal data secure and not disclosing it on purpose or accidentally to anybody who should not have access to the information. The Knares Medical Practice Basildon will provide training to staff if necessary. The Knares Medical Practice Basildon will consider in particular, the likelihood that personal data, including special categories of data, will be removed from The Knares Medical Practice Basildon's premises and taken to, for example, Patients' homes and residences. The Knares Medical Practice Basildon will ensure that all staff understand the importance of maintaining the confidentiality of personal data away from The Knares Medical Practice Basildon's premises and take care to ensure that the personal data is not left anywhere it could be viewed by a person who should not have access to that personal data.

4.15 The Knares Medical Practice Basildon will adopt policies and procedures in respect of recognising, resolving and reporting security incidents including breaches of GDPR. The Knares Medical Practice Basildon understands that it may need to report breaches to the ICO and to affected Data Subjects, as well as to CareCERT if The Knares Medical Practice Basildon is required to comply with the IG Toolkit and the new Data Security and Protection Toolkit.

4.16 The Knares Medical Practice Basildon will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data.

4.17 Privacy By Design

The Knares Medical Practice Basildon will take into account the GDPR requirements around privacy by design, particularly in terms of data security.

4.18 The Knares Medical Practice Basildon understands that privacy by design is an approach set out in GDPR that promotes compliance with privacy and data protection from the beginning of a project. The Knares Medical Practice Basildon will ensure that data protection and GDPR compliance is always at the forefront of the services it provides, and that it won't be treated as an afterthought.

4.19 The Knares Medical Practice Basildon will comply with privacy by design requirements by, for example:

- Identifying potential data protection and security issues at an early stage in any project or process, and addressing those issues early on; and
- Increasing awareness of privacy and data protection across The Knares Medical Practice Basildon, including in terms of updated policies and procedures adopted by The Knares Medical Practice Basildon

4.20 The Knares Medical Practice Basildon will conduct Privacy Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by The Knares Medical Practice Basildon. A template Privacy Impact Assessment will be provided in a future policy.

GDPR03 - Data Security and Data Retention Policy and Procedure

5. Procedure

5.1 The Knares Medical Practice Basildon will consider data retention and data security issues and concerns at the beginning of any project (whether the project is the introduction of a new IT system, a new way of working, the processing of a new type of personal data or anything else that may affect The Knares Medical Practice Basildon's processing activities). The Knares Medical Practice Basildon appreciates that this is key for complying with the privacy by design requirements in GDPR.

5.2 The Knares Medical Practice Basildon will review the periods for which it retains all the personal data that it processes.

5.3 The Knares Medical Practice Basildon will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all staff. The Knares Medical Practice Basildon will consider providing training to staff in respect of data retention.

5.4 The Knares Medical Practice Basildon will review the security measures currently in place in respect of all the personal data it processes.

5.5 The Knares Medical Practice Basildon will document the decisions it takes, and the logic and reasoning behind those decisions, in respect of both data retention and data security. The Knares Medical Practice Basildon will keep a record of all policies and procedures it implements to improve its compliance with GDPR.

6. Definitions

6.1 CareCERT

- The Care Computing Emergency Response Team, developed by NHS Digital. CareCERT offers advice and guidance to support health and social care organisations to respond to cyber security threats

6.2 Data Subject

- The individual about whom The Knares Medical Practice Basildon has collected personal data

6.3 Data Protection Act 1998 or DPA

- The law that relates to data protection in the UK. It will remain in force until and including 24 May 2018. It will be replaced by GDPR on 25 May 2018

6.4 GDPR

- The General Data Protection Regulation 2016. It will replace the Data Protection Act 1998 from 25 May 2018 as the law that governs data protection in the UK. It will come into force in the UK via the Data Protection Bill 2017

6.5 Personal Data

- Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, defined below

6.6 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data - at the point you collect it, you are processing it

6.7 Special Categories of Data

- Has an equivalent meaning to "Sensitive Personal Data" under the Data Protection Act 1998. Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views

GDPR03 - Data Security and Data Retention Policy and Procedure

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Anybody who processes personal data on behalf of The Knares Medical Practice Basildon should be made aware of and should comply with The Knares Medical Practice Basildon's policies in respect of data retention and data security

Key Facts - People Affected by The Service

People affected by this service should be aware of the following:

- The Knares Medical Practice Basildon will implement and embed the use of policies and procedures to ensure that all personal data processed about people affected by the services provided by The Knares Medical Practice Basildon, including Patients, is retained and is kept secure and protected in accordance with GDPR

Further Reading

There is no further reading for this policy, but we recommend the 'Underpinning Knowledge' section of the review sheet to increase your knowledge and understanding.

Outstanding Practice

To be outstanding in this policy area you could provide evidence that:

- You have reviewed the security measures in place in respect of the personal data The Knares Medical Practice Basildon processes and have determined whether those measures need updating. If further steps need to be taken to improve security, you have a plan in place to take those steps prior to 25 May 2018
- You have reviewed and considered the documents and guidance referenced in the "Underpinning Knowledge" and "Further Reading" sections
- You have considered the personal data you process and adopted and documented appropriate retention periods for each type of personal data
- The wide understanding of the policy is enabled by proactive use of the QCS App